

Figure 1.

Step 101

The **Sender** creates the message content (MailContent) and selects a random encryption key (SymmetricKey). Both MailContent and SymmetricKey should be kept by the **Sender** in order to verify the validity of the certified receipt later.

Step 102

The **Sender** sends to the **Recipient** the certified mail defined as:  
CertifiedMail = PKE(RemailerPublicKey, CertMailHeader) + CertMailBody  
where:  
CertMailHeader = MessageID + SymmetricKey;  
CertMailBody = HASH(SymmetricKey) + SKE(SymmetricKey, MailContent);  
MessageID = HASH(CertMailBody);

Step 103

After receiving CertifiedMail, the **Recipient** sends a receipt to the **Remailer**:  
ReceiptSentToRemailer = PKE(RemailerPublicKey, CertMailHeader) +  
HASH(SymmetricKey) + SignedReceipt  
Where: SignedReceipt = SIGNED(RecipientPrivateKey, MessageID2) and  
MessageID2 is the message ID the **Recipient** computed from the received  
message according to: MessageID2 = HASH(CertMailBody);

Step 104

The **Remailer** processes ReceiptSentToRemailer as the following:

- Decrypts PKE(RemailerPublicKey, CertMailHeader) to obtain SymmetricKey and MessageID from CertMailHeader.
- Verifies SignedReceipt using the public key of the **Recipient**.
- Verifies that MessageID obtained from CertMailHeader is exactly the same as MessageID2 in SignedReceipt.
- Verifies that HASH(SymmetricKey) in the ReceiptSentToRemailer agrees with the hash computed from SymmetricKey in CertMailHeader.
- If all the verifications succeed, send the SignedReceipt to the **Sender**.
- If sending receipt to the **Sender** succeeds, send the SymmetricKey to the **Recipient**.

Step 105

The **Recipient** decrypts SKE(SymmetricKey, MailContent) using the SymmetricKey received from the **Remailer** to obtain MailContent.

Step 106

After receiving the SignedReceipt, the **Sender** is able to prove that the recipient has received the exact MailContent by demonstrating:

- The **Recipient's** signature signed SignedReceipt can be verified using **Recipient's** public key.
- The MessageID2 in the SignedReceipt agrees with the hash of CertMailBody reconstructed from SymmetricKey and MailContent the **Sender** has kept.

Figure 2

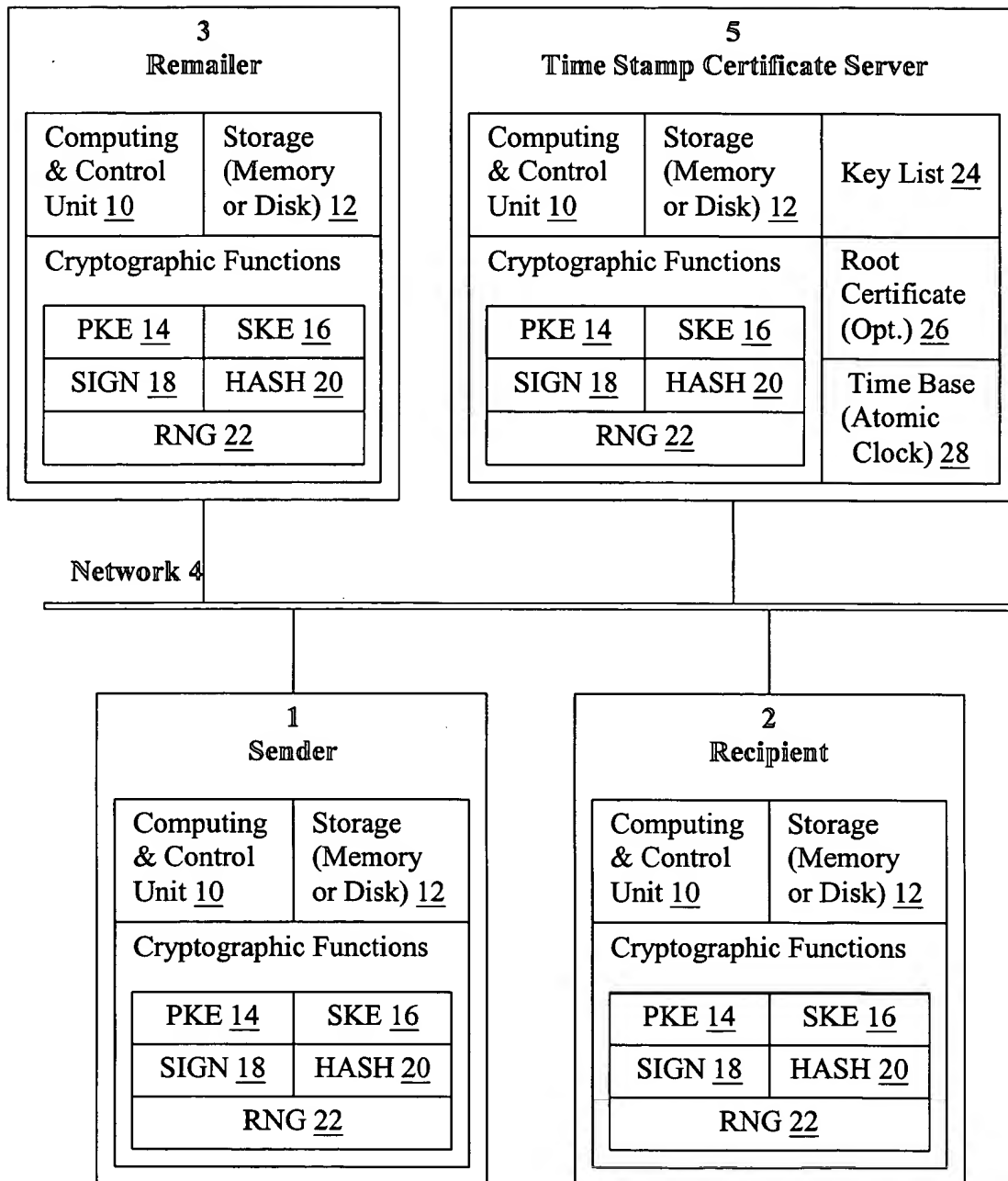
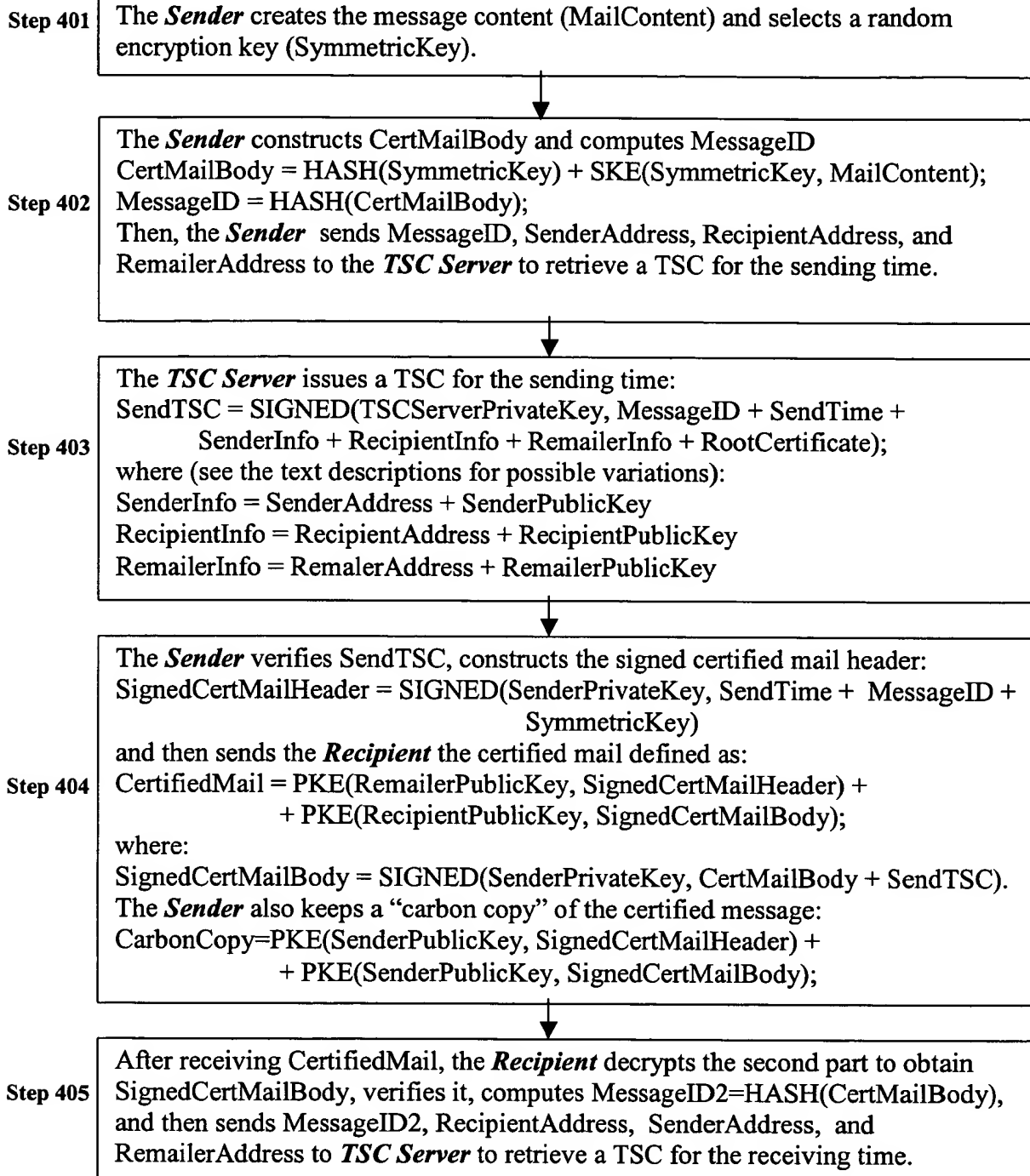


Figure 3.



Continued to Figure 4b

**Figure 4a**

Continued from Figure 4a

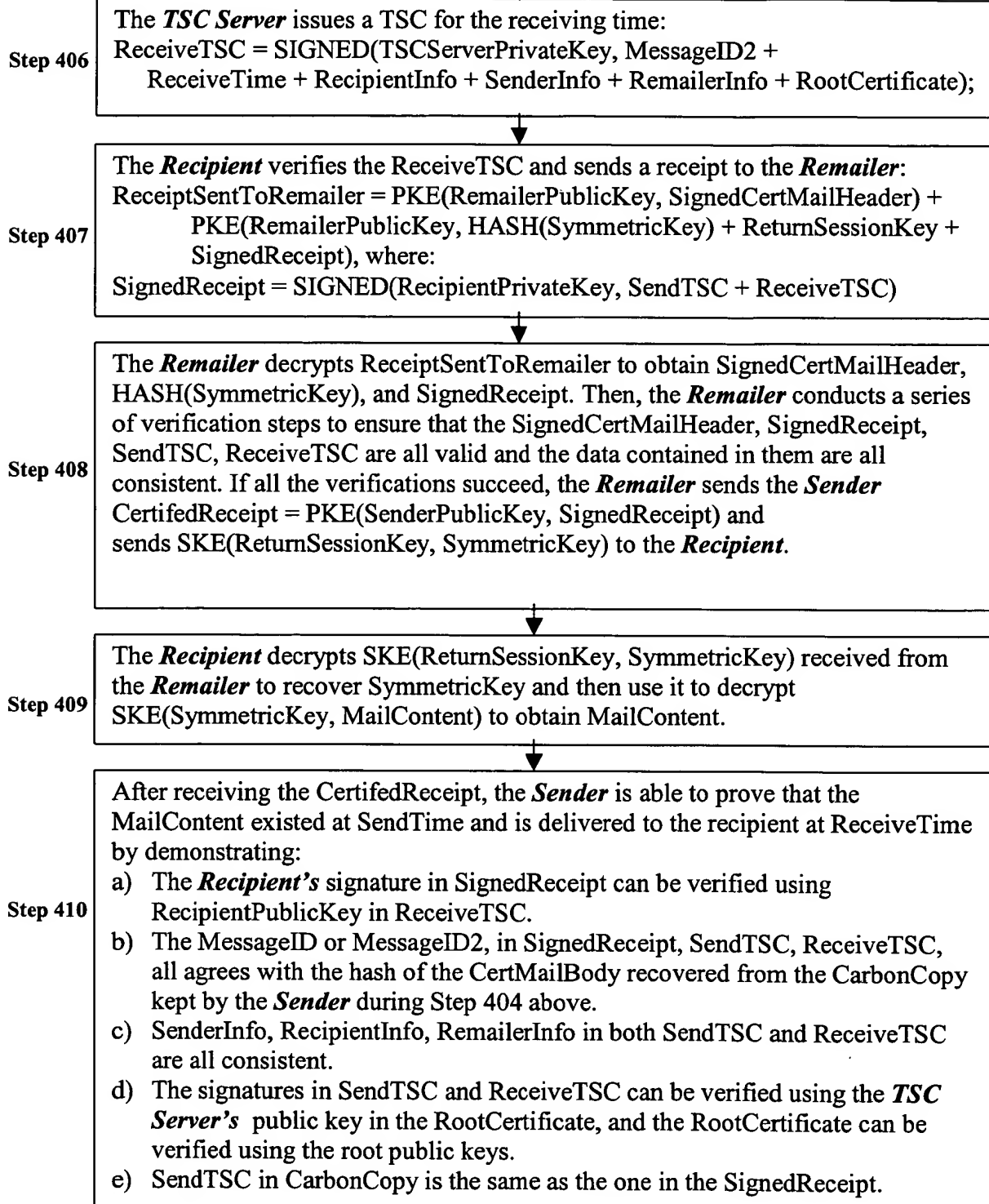


Figure 4b